WHAT IS CLAIMED IS:

1. A data processing system comprising:

a host computer system;

an interconnect coupled to the host computer system;

a storage array coupled to the interconnect and configured to store data received from the host computer system over the interconnect; and

a data integrity device coupled to the interconnect and comprising at least one processor, wherein the data integrity device is configured to be enabled and disabled;

wherein if the data integrity device is disabled, the host computer system and the storage array provide a first level of error protection for the data;

wherein if the data integrity device is enabled, the at least one processor is configured to perform a first data integrity operation on the data in order to provide a second level of error protection for the data in addition to the first level of error protection provided by the host computer system and the storage array.

2. The data processing system of claim 1, wherein the first data integrity operation comprises a checksum calculation.

3. The data processing system of claim 1, wherein the at least one processor is configured to perform the first data integrity operation by comparing a first checksum

corresponding to the data to a second checksum calculated from the data by the at least one processor.

4. The data processing system of claim 3, wherein the first checksum is transferred with the data.

5. The data processing system of claim 3, wherein the data integrity device is configured to provide an error indication if the first checksum does not equal the second checksum.

6. The data processing system of claim 1, wherein the data is encoded with an error correcting code, wherein as part of the first data integrity operation the data integrity device is configured to verify and correct the data using the error correcting code.

7. The data processing system of claim 1, wherein the data integrity device is configured to perform the first data integrity operation on the data as the data is written to the storage array.

8. The data processing system of claim 7, wherein in response to an indication that the data has been written to the storage array, the data integrity device is configured to perform a second data integrity operation on the data.

9. The data processing system of claim 7, wherein the data integrity device is configured to perform a second data integrity operation on the data as the data is read from the storage array.

10. The data processing system of claim 1, wherein the data integrity device comprises a plurality of processors, wherein the plurality of processors are each configured to perform the first data integrity operation on the data at a same time.

11. The data processing system of claim 1, wherein the data integrity device comprises a plurality of processors, wherein each of the plurality of processors is configured to be enabled independently of each of other processor in the plurality of processors.

12. The data processing system of claim 11, wherein a control function running on the host system is configured to allow a user to select how many of the plurality of processors are enabled.

13. The data processing system of claim 11, wherein if more than two of the plurality of processors are enabled, the data integrity device is configured to perform a voting operation on each of the enabled processors' results.

14. The data processing system of claim 13, wherein if a majority of the enabled processors generates a same result and a minority of the enabled processors generates a different result, the data integrity device is configured to provide an error indication indicating that an error occurred in the data integrity device.

15. The data processing system of claim 14, wherein the data integrity device is configured to disable the minority of the enabled processors that generate the different result.

16. The data processing system of claim 15, wherein the data integrity device comprises one or more redundant processors, wherein the data integrity device is configured to enable one of the redundant processors in response to disabling one of the minority of the enabled processors.

17. The data processing system of claim 14, wherein the data integrity device is configured to initiate diagnostic tests on the minority of the enabled processors that generate the different result.

18. The data processing system of claim 11, wherein if two of the plurality of processors are enabled, the data integrity device is configured to compare the enabled processors' results.

19. The data processing system of claim 1, wherein the storage array comprises a RAID (Redundant Array of Inexpensive Disks) array.

20. The data processing system of claim 17, wherein the storage array comprises an array controller configured to manage the RAID array, wherein the array controller is configured to perform a second data integrity operation on the data.

21. The data processing system of claim 1, wherein the storage array comprises a plurality of disk drives, wherein each disk drive comprises a controller, wherein each disk drive's controller is configured to perform a second data integrity operation on the data.

22. The data processing system of claim 1, wherein a file system running on the host system is configured to perform a second data integrity operation on the data.

23. The data processing system of claim 1, wherein the data integrity device comprises a memory configured to store instructions for performing the data integrity operation.

24. The data processing system of claim 23, wherein the host system is configured to update the instructions for performing the data integrity operation that are stored in the memory.

25. The data processing system of claim 1, wherein the data integrity device comprises a memory configured to store instructions for performing diagnostic tests on the at least one processor comprised in the data integrity device.

26. The data processing system of claim 1, wherein the data integrity device comprises a memory configured to buffer the data.

27. The data processing system of claim 26, wherein a write from the host system to the storage array comprises a plurality of data packets, wherein the data is a first data packet.

28. The data processing system of claim 27, wherein after initiating a transfer of the first packet to the storage array, the host system is configured to wait until the data integrity device has performed the data integrity operation on the first data packet before initiating a transfer of a second data packet.

29. The data processing system of claim 26, wherein a write from the host system to the storage array comprises a plurality of data packets, wherein the data comprises the plurality of data packets in the write.

30. The data processing system of claim 1, wherein the data integrity device comprises a memory and wherein the data integrity device is configured to store a result of the data integrity operation in the memory.

31. The data processing system of claim 1, wherein the data comprises a packet, wherein the host system is configured to insert one of a packet identification and a time stamp into the packet, wherein if the data integrity device detects an error in the packet, the data integrity device is configured to provide the one of the packet identification and the time stamp to the host system.

32. The data processing system of claim 1, wherein the data integrity device has an associated device identification, wherein the data integrity device is configured to provide its associated device identification if the data integrity device provides an error indication.

33. The data processing system of claim 1, wherein the data integrity device is configured to provide in-band error indications.

34. The data processing system of claim 1, wherein the data integrity device is configured to provide out-of-band error indications.

35. The data processing system of claim 1, wherein the data integrity device is implemented as a modular device that is configured to be inserted into the storage array.

36. The data processing system of claim 1, wherein the data integrity device is configured to be removable from the data processing system.

37. The data processing system of claim 1, wherein in response to the data integrity device being enabled, the host system is configured to reduce a rate at which the data is transferred on the interconnect.

38. The data processing system of claim 37, wherein the data integrity device comprises a plurality of processors, wherein an amount by which the rate is reduced depends on a number of the plurality of processors that are currently enabled in the data integrity device.

39. A data processing system comprising:

a host computer system;

a storage array;

an interconnect coupled to the host computer system and the storage array and configured to transfer data between the host computer system and the storage array; and

a data integrity device coupled to the interconnect and comprising a plurality of processors configured to be individually enabled or disabled by the host computer system, wherein each processor is configured to perform a data integrity operation on the data being transferred over the interconnect when that processor is enabled;

wherein a number of the processors enabled by the host computer system corresponds to a user-selected level of error protection.

40. A method of performing a data integrity operation comprising:

initiating a data transfer between a host computer system and a storage array;

a plurality of processors in a data integrity device each performing a data integrity operation on the data to generate a result in response to said initiating if the data integrity device is enabled; and

if the processors' results are equal and indicate that the data is erroneous, providing an indication that the data is erroneous to the host computer system.

41. The method of claim 40, wherein said performing comprises performing a checksum calculation on the data.

42. The method of claim 40, wherein said performing comprises capturing a first checksum transferred with the data and comparing the first checksum to a second checksum calculated from the data.

43. The method of claim 42, further comprising providing an error indication if the first checksum does not equal the second checksum.

44. The method of claim 40, wherein the data is encoded with an error correcting code, wherein said performing comprises verifying and correcting the data using the error correcting code.

45. The method of claim 40, said performing comprises performing the data integrity operation on the data as the data is written to the storage array.

46. The method of claim 40, wherein the data integrity device is configured to perform the data integrity operation on the data as the data is read from the storage array.

47. The method of claim 40, wherein said performing comprises the plurality of processors performing the data integrity operation on the data in lockstep.

48. The method of claim 40, further comprising performing a voting operation on the processors' results.

49. The method of claim 48, further comprising providing an error indication indicating that an error occurred in the data integrity device if a majority of the processors generates a same result and a minority of the processors generates a different result.

50. The method of claim 48, further comprising disabling the minority of the processors that generate the different result.

51. The method of claim 50, further comprising enabling one or more redundant processors in response to disabling one or more of the minority of the processors.

52. The method of claim 48, further comprising initiating diagnostic tests on the minority of the processors that generate the different result.

53. The method of claim 40, further comprising comparing the processors' results.

54. The method of claim 40, further comprising buffering the data in a memory comprised in the data integrity device.

55. The method of claim 54, wherein a write from the host computer system to the storage array comprises a plurality of data packets, wherein the data is a first data packet.

56. The method of claim 55, further comprising the host computer system waiting until said performing has had time to complete before initiating a transfer of a second data packet.

57. The method of claim 54, wherein a write from the host computer system to the storage array comprises a plurality of data packets, wherein the data comprises the plurality of data packets in the write.

58. The method of claim 40, wherein the data comprises a packet, wherein the method further comprises:

the host computer system inserting one of a packet identification and a time stamp into the packet; and

the data integrity device providing the one of the packet identification and the time stamp to the host system if the processors' results are equal and indicate that the packet is erroneous.

59. The method of claim 40, further comprising enabling the data integrity device and the host computer system reducing a rate at which the data is transferred on the interconnect in response to the data integrity device being enabled.

60. The method of claim 40, further comprising the host computer system disabling one or more of the processors.

61. The method of claim 40, further comprising the host computer system enabling the processors.

62. A method comprising:

performing a first data transfer between a host computer system and a storage array, wherein a data integrity device is disabled during said performing;

subsequent to said performing, enabling the data integrity device;

initiating a second data transfer between a host computer system and a storage array;

in response to said enabling and said initiating, one or more processors comprised in the data integrity device performing a data integrity operation on data transferred in the second data transfer.

63. The method of claim 62, wherein said enabling comprises the host computer system enabling a number of processors comprised in the data integrity device, wherein the number of processors corresponds to a user-selected level of error protection.

64. The method of claim 63, wherein if the number of processors is two, said performing a data integrity operation comprises:

two processors comprised in the data integrity device each performing the data integrity operation on the data transferred in the second data transfer to generate a result; and

a first processor comparing the two processors' results and generating an error indication if the two processors' results are not equal.

65. The method of claim 63, wherein if the number of processors is greater than two, said performing a data integrity operation comprises:

three or more processors comprised in the data integrity device each performing the data integrity operation on the data transferred in the second data transfer to generate a result;

a first processor performing a voting operation on the three or more processors' results and generating an error indication if the three or more processors' results are not equal.

66. A data integrity device comprising:

an interface configured to receive data being transferred in a storage system; and

one or more processors coupled to receive the data from the interface and configured to perform a data integrity operation on the data;

wherein at least one of the one or more processors is configured to provide an indication if an error is detected in the data; and

wherein the one or more processors are configured to be enabled and disabled.

67. A data processing system comprising:

host computing means for processing data;

storage means for storing the data;

communication means for communicating the data from the host computing means to the storage means, wherein the communication means are coupled to the host computing means and the storage means;

means for performing a data integrity operation on the data communicated on the communication means and responsive to various settings, wherein one of the settings disables the means for performing the data integrity operation;

wherein if the means for performing the data integrity operation are disabled, the host computing means and the storage means provide a first level of error protection for the data;

wherein if the means for performing the data integrity operation are enabled, the means perform the data integrity operation on the data in order to provide a second level of error protection for the data in addition to the first level

of error protection provided by the host computing means and the storage means.